Classical and Quantum Polynomial Reconstruction via Legendre Symbol Evaluation

Alexander Russell
Department of Computer Science and Engineering
University of Connecticut, Storrs, CT 06269 USA
acr@cse.uconn.edu

Igor E. Shparlinski
Department of Computing
Macquarie University, Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

December 4, 2002

Abstract

We consider the problem of recovering a hidden monic polynomial $f(X)$ of degree $d \geq 1$ over a finite field $\mathbb{F}_p$ of p elements given a black box which, for any $x \in \mathbb{F}_p$, evaluates the quadratic character of $f(x)$. We design a classical algorithm of complexity $O(d^2 p^{d+\varepsilon})$ and also show that the quantum query complexity of this problem is $O(d)$. Some of our results extend those of Wim van Dam, Sean Hallgren and Lawrence Ip obtained in the case of a linear polynomial $f(X) = X + s$ (with unknown s); some are new even in this case.

1 Introduction

Let $p \geq 3$ be a prime number and let $\mathbb{F}_p$ denote a finite field of p elements. We let χ denote the quadratic character of $\mathbb{F}_p$, or the *Legendre symbol* modulo p; see [17].

Wim van Dam, Sean Hallgren and Lawrence Ip, in the series of papers [4, 5, 6, 14] have considered the *shifted Legendre symbol* problem of finding an unknown shift $s \in \mathbb{F}_p$ given an oracle $\mathcal{O}$ which for each $x \in \mathbb{F}_p$ computes $\chi(x+s)$. They have designed efficient quantum algorithms for the above problem and its generalisation to characters in residue rings.

The problem is of intrinsic interest and also has strong cryptographic motivation; sequences of values of quadratic characters have been considered as sources of cryptographically strong pseudorandom bits [2, 3, 7, 10, 13, 18, 19, 21, 22].

Here we consider a generalisation of the above problem to polynomials.

For an integer d we let $\mathcal{M}_d$ denote the set of square-free monic polynomials $f(X) \in \mathbb{F}_p[X]$ of degree d,

$$\mathcal{M}_d \stackrel{\Delta}{=} \left\{ f(X) = X^d + s_{d-1}X^{d-1} + \ldots + s_1 X + s_0 \mid s_i \in \mathbb{F}_p \right\}.$$

We study the problem of finding $f \in \mathcal{M}_d$, given an oracle $\mathcal{O}_f$ which returns $\chi(f(x))$ for any $x \in \mathbb{F}_p$:

$$\mathcal{O}_f : x \mapsto \chi(f(x)).$$

It is obvious that the square-freeness condition is essential because polynomials of the form $f_1(X) = F(X)G_1(X)^2$ and $f_1(X) = F(X)G_2(X)^2$ with $F(X), G_1(X), G_2(X) \in \mathbb{F}_p[X]$ cannot be distinguished by this oracle.

We remark that for the approach of [4, 5, 6, 14] the orthogonality condition

$$\sum_{x \in \mathbb{F}_p} \chi\left((x+a)(x+b)\right) = \begin{cases} p-1, & \text{if } a = b, \\ -1, & \text{if } a \neq b, \end{cases} \qquad a, b \in \mathbb{F}_p,$$

appears to be crucial, however, this condition fails for nonlinear polynomials. On the other hand, the *Weil bound*, see [17], provides a certain approximate analogue of the above identity:

$$\sum_{x \in \mathbb{F}_p} \chi\left(g(x)h(x)\right) = \begin{cases} p + O(d), & \text{if } g = h, \\ O(p^{1/2}), & \text{if } g \neq h, \end{cases} \qquad g, h \in \mathcal{M}_d. \tag{1}$$

Hereafter the implied constants in symbols 'O' may depend on d and also, where obvious, on the small positive parameter ε.

Using this property we demonstrate that the quantum query complexity of recovering f, given the oracle $\mathcal{O}_f$, is $O(d)$. In contrast, we observe that the classical query complexity is $\Omega(d \log p)$. Furthermore, we give a classical algorithm for reconstructing f from $\mathcal{O}_f$, which appears to be new even in the case of linear polynomials. In fact this algorithm is also based on the Weil bound.

It is clear that the brute force approach leads to a (classical) algorithm of complexity $O(p^{d+1+\varepsilon})$ which is based on computation and comparison of the p-dimensional vectors of the values of $\chi(f(x))$ and $\chi(g(x))$ for all $x \in \mathbb{F}_p$ and all $g \in \mathcal{M}_d$. A naive use of the Weil bound shows that it is enough to compute and compare $\chi(f(x))$ and $\chi(g(x))$ only for $1 \le x \le dp^{1/2} \log^2 p$ which leads to an algorithm of complexity $O(p^{d+1/2+\varepsilon})$. We show that using the Weil bound in a less obvious way one can obtain an $O(p^{d+\varepsilon})$ algorithm.

It could be relevant to recall the work of Dima Grigoriev [12] where a somewhat related question is considered for multivariate polynomials (although the field characteristic is assumed to be small).

It is easy to see that our method applies to multiplicative characters of other orders and to multivariate polynomials as well.

Finally, it is also easy to see that we can allow oracles which return the right value of $\chi(f(x))$ only with some fixed probability $\gamma > 1/2$. We do not pursue this issue in this work, though.

Acknowledgement. We thank Asma Harcharras for several useful discussions.

2 Preparation

First of all we recall the Weil bound in its classical form given in Example 12 of Appendix 5 of [24]; see also Theorem 3 of Chapter 6 in [16] and Theorem 5.41 and comments to Chapter 5 of [17].

Lemma 1. *For any $F \in \mathcal{M}_d$ which is not a perfect square of another poly-*

nomial, the bound

$$\left|\sum_{x\in\mathbb{F}_p}\chi\left(F(x)\right)\right| \le dp^{1/2}$$

holds.

The following statement is also implied by the Weil bound and is essentially Theorem 2 of [19].

Lemma 2. *For any integers $M < p$ and any $F \in \mathcal{M}_d$ which is not a perfect square of another polynomial, the bound*

$$\left|\sum_{x=1}^{M}\chi(F(x))\right| = O\left(dp^{1/2}\log p\right)$$

holds.

We also need a similar statement for multivariate polynomials.

Lemma 3. *For any collection of ℓ pairwise distinct linear forms*

$$L_\nu\left(S_0,\dots,S_{d-1}\right) = S_0 + S_1c_{1\nu} + \ldots + S_{d-1}c_{d-1,\nu} + c_{d,\nu}, \qquad \nu = 1,\dots,\ell,$$

over $\mathbb{F}_p$ the bound

$$\left|\sum_{s_0,\dots,s_{d-1}\in\mathbb{F}_p}\chi\left(\prod_{\nu=1}^{\ell}L_\nu(s_0,\dots,s_{d-1})\right)\right| \le 2\ell p^{d-1/2}$$

holds.

Proof. We have

$$\left|\sum_{s_0,\dots,s_{d-1}\in\mathbb{F}_p}\chi\left(\prod_{\nu=1}^{\ell}L_\nu(s_0,\dots,s_{d-1})\right)\right| \le \sum_{s_1,\dots,s_{d-1}\in\mathbb{F}_p}\left|\sum_{s_0\in\mathbb{F}_p}\chi\left(\prod_{\nu=1}^{\ell}L_\nu(s_0,\dots,s_{d-1})\right)\right|.$$

Clearly, there are at most

$$\frac{(\ell-1)(\ell-2)}{2}p^{d-2} \le \ell 2p^{d-2}$$

$d-1$-tuples $(s_1 \dots, s_{d-1}) \in \mathbb{F}_p$ for which the values of

$$s_1c_{1\nu} + \ldots + s_{d-1}c_{d-1,\nu} + c_{d,\nu}, \qquad \nu = 1, \dots, \ell,$$

are pairwise distinct. In this case we estimate the sum over s_0 by p. Otherwise we see from Lemma 1 that the sum over s_0 does not exceed $\ell p^{1/2}$. Therefore

$$\left| \sum_{s_0,\dots,s_{d-1} \in \mathbb{F}_p} \chi\left(\prod_{\nu=1}^{\ell} L_\nu(s_0, \dots, s_{d-1})\right)\right| \le \ell p^{d-1/2} + \ell 2p^{d-1}.$$

The claimed bound is trivial for $\ell \ge p^{1/2}$, otherwise we have $\ell p^{d-1/2} \ge \ell 2p^{d-1}$ and the result follows. □

We remark that one can also use stronger bounds based on the famous results of Pierre Deligne [8, 9], however they do improve our final results.

Our next statement gives an upper bound "on average" for weighted character sums with polynomials.

Lemma 4. *For any integers $N \le p$, $r \ge 1$ and any sequence of real numbers α_x with $|\alpha_x| \le 1$, $x = 1, \dots, N$, the bound*

$$\sum_{g \in \mathcal{M}_d} \left| \sum_{x \in \mathbb{F}_p} \alpha_x \chi\left(g(x)\right)\right|^{2r} \le 4rN^{2r}p^{d-1/2} + \frac{(2r)!}{r!}N^r p^d$$

holds.

Proof. We have

$$\begin{aligned}
\sum_{g \in \mathcal{M}_d} \left| \sum_{x \in \mathbb{F}_p} \alpha_x \chi\left(g(x)\right)\right|^{2r} &= \sum_{g \in \mathcal{M}_d} \sum_{x_1,\dots,x_{2r} \in \mathbb{F}_p} \prod_{i=1}^{2r} \alpha_{x_i} \chi\left(g(x_i)\right) \\
&= \sum_{x_1,\dots,x_{2r} \in \mathbb{F}_p} \prod_{i=1}^{2r} \alpha_{x_i} \sum_{g \in \mathcal{M}_d} \chi\left(\prod_{i=1}^{2r} g(x_i)\right) \\
&= \sum_{x_1,\dots,x_{2r} \in \mathbb{F}_p} \left| \sum_{g \in \mathcal{M}_d} \chi\left(\prod_{i=1}^{2r} g(x_i)\right)\right|.
\end{aligned}$$

Assume that $x_1, \ldots, x_{2r} \in [1, N]$ contains m pairs of equal elements

$$x_{i_\nu} = x_{j_\nu}, \qquad \nu = 1, \ldots, m,$$

and $l = 2r - 2m$ pairwise distinct elements $y_\nu = x_{k_\nu}$, $\nu = 1, \ldots, m$. Then

$$\sum_{g \in \mathcal{M}_d} \chi\left(\prod_{i=1}^{2r} g(x_i)\right) = \sum_{g \in \mathcal{M}_d} \chi\left(\prod_{\nu=1}^{l} g(y_\nu)\right).$$

If $l = 0$, which happens for at most

$$r!2r()rN^r = \frac{(2r)!}{r!}N^r$$

$2r$-tuples $(x_1, \ldots, x_{2r}) \in [1, N]^{2r}$, then the sum over g is obviously equal to $|\mathcal{M}_d| = p^d$. For $l > 0$ we derive

$$\sum_{g \in \mathcal{M}_d} \chi\left(\prod_{\nu=1}^{l} g(y_\nu)\right) = \sum_{s_0, \ldots, s_{d-1}} \chi\left(\prod_{\nu=1}^{l} \left(s_0 + s_1 y_\nu + \ldots + s_{d-1} y_\nu^{d-1} + y_\nu^d\right)\right).$$

It is easy to verify that because $y_1, \ldots, y_l$ are pairwise distinct elements of $\mathbb{F}_p$ the linear forms

$$S_0 + S_1 y_\nu + \ldots + S_{d-1} y_\nu^{d-1} + y_\nu^d, \qquad \nu = 1, \ldots, m,$$

satisfy the conditions of Lemma 3. Thus for at most N^{2r} remaining $2r$-tuples $(x_1, \ldots, x_{2r}) \in [1, N]^{2r}$ the sum over g is at most $2lp^{d-1/2} \le 4rp^{d-1/2}$ □

We recall that, using the Horner scheme, for any $g \in \mathcal{M}_d$ the value of $g(x)$ can be computed with $O(d)$ arithmetic operations modulo p. We also recall that polynomial evaluation and computing the quadratic character can be done in polynomial time in the standard RAM model of computation. Explicit and efficient versions of these statements can be found in [1, 11].

3 Classical Algorithm

Here we design an algorithm for the classical model of computation on a RAM computer. The complexity of our algorithm can be improved slightly if one uses fast algorithms for finite field arithmetic and polynomial evaluation, see [1, 11]. In particular, one can replace p^ε by a reasonably small power of $\log p$ and also improve the term d^2 in our estimate.

Theorem 5. *For any fixed $\varepsilon > 0$ and $d \ge 1$, given an oracle $\mathcal{O}_f$ one can find $f \in \mathcal{M}_d$ in $O\left(d^2 p^{d+\varepsilon}\right)$ binary operations.*

Proof. Obviously we can assume that p is sufficiently large. Put $M = \left\lceil dp^{1/2} \log^2 p \right\rceil$ and $N = \left\lceil d \log^2 p \right\rceil$.

Using the square-freeness condition we conclude that for any $g \in \mathcal{M}_d$ with $g \ne f$ the polynomial gf is not a prefect square. Thus from Lemma 2 we see that in this case

$$\sum_{x=1}^{M} \chi(g(x)f(x)) = O(M/\log p)$$

while for $g = f$ this sum is at least $M - d$. Using the Horner scheme, for any any $g \in \mathcal{M}_d$ the value of $g(x)$ can be computed with $O(d)$ arithmetic operations modulo p. Thus for any polynomial $g \in \mathcal{M}_d$ the above sum can be evaluated and the identity $g = f$ can be verified in $O(d^2 p^{1/2+\varepsilon})$ binary operations. We now show that in fact for all, except at most $O(p^{d-1/2} \log p)$ polynomials $g \in \mathcal{M}_d$ one can verify the identity $g = f$ in $O(dN \log^2 p)$ binary operations. It is enough to show that that the inequality

$$\left| \sum_{x=1}^{N} \chi(g(x)f(x)) \right| \ge N - d \tag{2}$$

is possible for at most $O(p^{d-1/2} \log p)$ polynomials $g \in \mathcal{M}_d$. Using Lemma 4 with $\alpha_x = \chi(f(x))$, we see that the number T of polynomials $g \in \mathcal{M}_d$ with (2), for any integer $r \ge 1$, satisfies the inequality

$$T(N-d)^{2r} \le 4rN^{2r}p^{d-1/2} + \frac{(2r)!}{r!}N^r p^d.$$

Let $r = \lceil \log p \rceil$. We have

$$(N-d)^{2r} \ge N^{2r}(1-d/N)^{2r} \ge N^{2r}/2$$

for sufficiently large p. Therefore

$$T \le 8rp^{d-1/2} + 2\frac{(2r)!}{r!}N^{-r}p^d \le 8rp^{d-1/2} + 2(2r)^r N^{-r} p^d.$$

Taking into account that $(2r)^r N^{-r} = (2r/N)^{-r} \le p^{-1/2}$ for our choice of N and r, and sufficiently large p, we obtain the desired statement. □

4 Quantum Query Complexity

As above, we consider the problem of recovering a polynomial f from an oracle $\mathcal{O}_f : x \mapsto \chi(f(x))$. An easy counting argument shows that the classical query complexity is $\Omega(d \log p)$ (it is in fact $\Theta(d \log p)$): see, for example, van Dam's article [4], for an analogous argument. We begin by showing that the quantum query complexity of this problem is at most $O(d)$. We refer the reader to accounts by Nielson and Chuang [20] and Kitaev [15] for a discussion of quantum computation and quantum algorithms. In particular, we need the notion of positive operator valued measurement (POVM) (see, e.g., [23], for a discussion which matches our notation below).

Recall that a POVM P on Hilbert space $\mathcal{H}$ is a set $\mathcal{A}$ and a family $\{\vartheta_a \mid a \in \mathcal{A}\}$ of positive semidefinite operators on $\mathcal{H}$ with the property that

$$\sum_{a \in \mathcal{A}} \vartheta_a = \iota,$$

where ι denotes the identity operator. The result of the measurement P on the state $\Psi \in \mathcal{H}$ is the probability distribution on $\mathcal{A}$ where $a \in \mathcal{A}$ is observed with probability $\langle \vartheta_a \Psi, \Psi \rangle$. Note that $\langle \vartheta_a \Psi, \Psi \rangle \geq 0$, as ϑ_α is positive semidefinite, and that

$$\sum_{a \in \mathcal{A}} \langle \vartheta_a \Psi, \Psi \rangle = \left\langle \sum_{a \in \mathcal{A}} \vartheta_a \Psi, \Psi \right\rangle = \langle \iota \Psi, \Psi \rangle = \|\Psi\|^2 = 1.$$

Note, also, that in the special case when $\vartheta_a = \gamma \pi$ for a projection π and a scalar $\gamma \in [0, 1]$, $\langle \vartheta_a \Psi, \Psi \rangle = \gamma \|\pi \Psi\|^2$.

Theorem 6. *Let f be a polynomial in $\mathcal{M}_d$. If $d \leq p^{1/2-\varepsilon}$ for some fixed $\varepsilon > 0$ then there exists a quantum algorithm which, after $O(d)$ quantum queries to $\mathcal{O}_f$, produces a state for which there is a POVM that determines f with probability at least $1 + O(p^{-1})$.*

Proof. Let us put $k = \lceil 2(d+1)\varepsilon^{-1} \rceil$. For a prime p, let $\mathcal{G}$ denote a p-dimensional Hilbert space with an orthonormal basis $\{|z\rangle \mid z \in \mathbb{Z}_p\}$. Initially, by applying the Fourier transform to a delta state, we arrive at the uniform superposition

$$\Upsilon \triangleq \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} |x\rangle \in \mathcal{G}$$

which is used to query the oracle O_f. Let $\widetilde{\chi} : \mathbb{F}_p \to \{\pm 1\}$ be the function

$$\widetilde{\chi}(x) = \begin{cases} \chi(x) & \text{if } x \neq 0, \\ 1 & \text{if } x = 0. \end{cases}$$

We can certainly assume that in fact we are given an oracle $\widetilde{\mathcal{O}_f}$ with $\widetilde{\mathcal{O}_f}(x) = \widetilde{\chi}(f(x))$. Then the result of the query may be computed into the phases by controlled phase shift yielding the state

$$\Psi_f \stackrel{\Delta}{=} \frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} \widetilde{\chi}(f(x)) \, |x\rangle \, .$$

Repeating the process independently $k \geq 1$ times yields the tensor product state

$$\Psi_{f,k} \stackrel{\Delta}{=} \frac{1}{p^{k/2}} \sum_{\mathbf{x} \in \mathbb{F}_p^k} \left(\prod_{i=1}^{k} \widetilde{\chi}(f(x_i)) \right) |\mathbf{x}\rangle \in \mathcal{G}^{\otimes k}$$

where $\mathbf{x} = (x_1, \ldots, x_k)$,

$$\mathcal{G}^{\otimes k} \stackrel{\Delta}{=} \underbrace{\mathcal{G} \otimes \cdots \otimes \mathcal{G}}_{k},$$

and $|\mathbf{x}\rangle \stackrel{\Delta}{=} |x_1\rangle \otimes \cdots \otimes |x_k\rangle$. In general, we let $\Psi_{g,k}$ denote the state that would have arisen at this point had we started with the polynomial $g \in \mathcal{M}_d$. Observe that for $g \in \mathcal{M}_d$, $\langle \Psi_{g,k}, \Psi_{g,k} \rangle = 1$ and, furthermore, that for distinct $g, h \in \mathcal{M}_d$,

$$\begin{aligned} |\langle \Psi_{g,k}, \Psi_{h,k} \rangle| &= \frac{1}{p^k} \left| \sum_{\mathbf{x} \in \mathbb{F}_p^k} \prod_{i=1}^{k} \widetilde{\chi}(g(x_i)) \widetilde{\chi}(h(x_i)) \right| \\ &= \frac{1}{p^k} \prod_{i=1}^{k} \left| \sum_{z \in \mathbb{F}_p} \widetilde{\chi}(g(z)) \widetilde{\chi}(h(z)) \right| . \end{aligned}$$

To bound this, we focus on the inner quantity

$$\sigma_{2d} \stackrel{\Delta}{=} \max_{\substack{g,h \in \mathcal{M}_d \\ g \neq h}} \left| \sum_{z \in \mathbb{F}_p} \widetilde{\chi}(g(z)) \widetilde{\chi}(h(z)) \right| .$$

For a polynomial $g \in \mathbb{F}_p[X]$, let $\mathcal{V}(g) = \{x \in \mathbb{F}_p \mid g(x) = 0\}$. Recall that $\mathcal{V}(gh) = \mathcal{V}(g) \cup \mathcal{V}(h)$ and that for a nonzero univariate polynomial g, $|\mathcal{V}(g)| \leq \deg(g)$. Considering that $\widetilde{\chi}(f(x)) = \chi(f(x))$ for $x \notin \mathcal{V}(f)$, we bound σ_{2d} as follows:

$$\begin{aligned}
\sigma_{2d} &= \max_{\substack{g,h \in \mathcal{M}_d \\ g \neq h}} \left| \sum_{z \in \mathbb{F}_p \setminus \mathcal{V}(gh)} \chi(g(z))\chi(h(z)) + \sum_{z \in \mathcal{V}(gh)} \widetilde{\chi}(g(z))\widetilde{\chi}(h(z)) \right| \\
&\leq \max_{\substack{g,h \in \mathcal{M}_d \\ g \neq h}} \left(\left| \sum_{z \in \mathbb{F}_p \setminus \mathcal{V}(gh)} \chi(gh(z)) \right| + |\mathcal{V}(gh)| \right) \\
&\leq \max_{\substack{g,h \in \mathcal{M}_d \\ g \neq h}} \left| \sum_{z \in \mathbb{F}_p} \chi(gh(z)) \right| + 2d.
\end{aligned}$$

Note now that for two distinct elements $g, h \in \mathcal{M}_d$, the product gh cannot be a perfect square and from Lemma 1 we conclude that

$$\sigma_{2d} \leq \max_{g \in \mathcal{M}_{2d}} \left| \sum_{z \in \mathbb{F}_p} \chi(g(z)) \right| + 2d \leq dp^{1/2} + 2d \leq 2dp^{1/2} \tag{3}$$

provided that $p > 3$ (otherwise the result is trivial). Hence for distinct $g, h \in \mathcal{M}_d$ we have

$$|\langle \Psi_{g,k}, \Psi_{h,k} \rangle| \leq \sigma_{2d}^k p^{-k}. \tag{4}$$

Now we show that there is a POVM that identifies the polynomial f with probability $1 + O(p^{-1})$. For each $g \in \mathcal{M}_d$, let $\pi_{g,k}$ be the projection operator onto the subspace spanned by $\Psi_{g,k}$. As each $\pi_{g,k}$ is a projection operator, it is positive semidefinite, and we now show that for some $0 < \alpha < 1$ with $\alpha = 1 + O(p^{-1})$, there is a decomposition of the identity operator ι of the form

$$\iota = \rho + \sum_{g \in \mathcal{M}_d} \alpha \pi_{g,k}$$

where ρ and all $\pi_{g,k}$ are positive semidefinite operators on $\mathcal{G}^{\otimes k}$. Note that if $\Psi_{f,k}$ is measured according to this POVM, the "correct" index f, k is observed with probability α.

So define $\rho = \iota - \sum_{g\in\mathcal{M}_d} \alpha\pi_{g,k}$; we wish to select $\alpha = 1+O(p^{-1})$ to insure that ρ is positive semidefinite. It suffices to see that for our choice of α

$$\left\| \sum_{g\in\mathcal{M}_d} \alpha\pi_{g,k} \right\| < 1, \tag{5}$$

where $\|M\|$ denotes the *operator norm* of M, given by

$$\|M\| \triangleq \sup_{\Phi\neq\mathbf{0}} \frac{\|M\Phi\|}{\|\Phi\|},$$

this supremum taken over all nonzero vectors Φ. Note that for a unit vector $\Phi \in \mathcal{G}^{\otimes k}$,

$$\sum_{g\in\mathcal{M}_d} \pi_{g,k}\Phi = \sum_{g\in\mathcal{M}_d} \langle \Phi, \Psi_{g,k}\rangle \Psi_{g,k}.$$

Let $\mathcal{F}_d$ be a Hilbert space of dimension $|\mathcal{M}_d|$ with orthonormal basis $\{\mathrm{B}_g \mid g \in \mathcal{M}_d\}$ and let $\tau : \mathcal{G}^{\otimes k} \to \mathcal{F}_d$ be the linear operator

$$\tau \triangleq \sum_{g\in\mathcal{M}_d} \Psi_g \mathrm{B}_g^*;$$

here $\mathrm{B}_g^* : \mathcal{F}_d \to \mathbb{C}$ is the linear functional $\mathrm{B}_g^* : \Phi \mapsto \langle \Phi, \mathrm{B}_g\rangle$. Then

$$\tau\tau^*(\Phi) = \sum_{g,h\in\mathcal{M}_d} \Psi_g \mathrm{B}_g^* \left(\mathrm{B}_h \Psi_h^*(\Phi)\right) = \sum_{g\in\mathcal{M}_d} \Psi_g \Psi_g^*(\Phi) = \sum_{g\in\mathcal{M}_d} \pi_{g,k}\Phi,$$

so that $\sum_g \pi_{g,k} = \tau\tau^*$; recalling that $\|\tau^*\|^2 = \|\tau\tau^*\|$, it suffices to suitably upper bound $\|\tau^*\|$. So let $\Phi \in \mathcal{G}^{\otimes k}$ be an element in the span of $\{\Psi_{g,k} \mid g \in \mathcal{M}_d\}$ and let $\Gamma = \sum_g \gamma_g \mathrm{B}_g \in \mathcal{F}_d$ satisfy $\tau(\Gamma) = \Phi$, which is to say that

$$\Phi = \sum_{g\in\mathcal{M}_d} \gamma_g \Psi_{g,k}.$$

Observe that

$$\begin{aligned} \|\Phi\|^2 &= \left\| \sum_{g\in\mathcal{M}_d} \gamma_g \Psi_{g,k} \right\|^2 = \sum_{g,h\in\mathcal{M}_d} \gamma_g \gamma_h^* \langle \Psi_{g,k}, \Psi_{h,k}\rangle \\ &= \sum_{g\in\mathcal{M}_d} |\gamma_g|^2 + O\left(\frac{\sigma_{2d}^k}{p^k} \left(\sum_{g\in\mathcal{M}_d} |\gamma_g| \right)^2 \right) \\ &= \|\Gamma\|^2 + O\left(\frac{\sigma_{2d}^k}{p^k} \left(p^d \|\Gamma\|^2 \right) \right) = \left(1 + O\left(p^{d-k}\sigma_{2d}^k\right)\right) \|\Gamma\|^2, \end{aligned} \tag{6}$$

by the Cauchy–Schwarz inequality. With Φ expressed in this way, we expand $\|\tau^*\Phi\|$ as follows:

$$\begin{aligned}\|\tau^*\Phi\|^2 &= \sum_{g\in\mathcal{M}_d} |\langle\Phi,\Psi_{g,k}\rangle|^2 = \sum_{g\in\mathcal{M}_d} \left|\left\langle \sum_{h\in\mathcal{M}_d} \gamma_h\Psi_{h,k},\Psi_{g,k}\right\rangle\right|^2 \\ &= \sum_{g\in\mathcal{M}_d} \left|\gamma_g + \sum_{h\neq g} \gamma_h\langle\Psi_{h,k},\Psi_{g,k}\rangle\right|^2 .\end{aligned} \tag{7}$$

Recalling the inner product bounds of (4), for any $g\in\mathcal{M}_d$ we must have

$$\left|\sum_{\substack{h\in\mathcal{M}_d\\ g\neq h}} \gamma_h\langle\Psi_{h,k},\Psi_{g,k}\rangle\right| \leq \sigma_{2d}^k p^{-k} \sum_{h\in\mathcal{M}_d} |\gamma_h| \leq \sigma_{2d}^k p^{-k}\sqrt{p^d}\,\|\Gamma\|\,, \tag{8}$$

again by the Cauchy–Schwarz inequality. Finally, considering that $\|\alpha+\beta\| \leq \|\alpha\|+\|\beta\|$, we conclude from (7) and (8) that

$$\|\tau^*\Phi\| \leq \|\Gamma\| + p^{d-k}\sigma_{2d}^k\,\|\Gamma\| = \left(1+p^{d-k}\sigma_{2d}^k\right)\|\Gamma\|$$

and, from (6), that

$$\|\tau^*\Phi\| \leq \left(1+O\left(p^{d-k}\sigma_{2d}^k\right)\right)\|\Phi\|\,.$$

Hence

$$\left\|\sum_{g\in\mathcal{M}_d}\pi_{g,k}\right\| \leq 1+O\left(p^{d-k}\sigma_{2d}^k\right).$$

We can assume that $p>2^{2/\varepsilon}$ and hence that $2\leq p^{\varepsilon/2}$, because otherwise the result is trivial. Then by (3) we have

$$p^{d-k}\sigma_{2d}^k \leq p^{d-k}\left(2dp^{1/2}\right)^k \leq p^{d-k}p^{(1-\varepsilon/2)k} = p^{d-k\varepsilon/2} \leq p^{-1},$$

because of our choice of k. We obtain

$$\left\|\sum_{g\in\mathcal{M}_d}\pi_{g,k}\right\| \leq 1+O\left(p^{-1}\right),$$

and are guaranteed that (5) holds (provided that p is large enough) for some $\alpha = 1+O(p^{-1})$ (recall that $(1+\delta)^{-1} = 1+O(\delta)$). Thus the above POVM determines f with probability $\alpha = 1+O(p^{-1})$. □

References

[1] A. V. Aho, J. E. Hopcroft and J. D. Ullman, *The Design and the Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[2] M. Anshel and D. Goldfeld, 'Zeta functions, one-way functions, and pseudorandom number generators', *Duke Math. J.*, **88** (1997), 371–390.

[3] D. Boneh and R. Lipton, 'Algorithms for black-box fields and their applications to cryptography', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **1109** (1996), 283–297.

[4] W. van Dam, 'Quantum algorithms for weighing matrices and quadratic residues', *Algorithmica*, **34** (2002).

[5] W. van Dam, and S. Hallgren, 'Efficient quantum algorithms for shifted quadratic character problem', *Preprint*, 2001, 1–15.

[6] W. van Dam, S. Hallgren and L. Ip, 'Quantum algorithms for hidden coset problems', *Preprint*, 2001, 1–10.

[7] I. B. Damgård, 'On the randomness of Legendre and Jacobi sequences', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **403** (1990), 163–172.

[8] P. Deligne, 'La conjecture de Weil, I' *Inst. Hautes Estudes Sci. Publ. Math.*, **43** (1974), 273–307.

[9] P. Deligne, 'La conjecture de Weil, II' *Inst. Hautes Estudes Sci. Publ. Math.*, **52** (1981), 313–428.

[10] C. Ding, 'Pattern distributions of Legendre sequences', *IEEE Trans. Inform. Theory*, **44** (1998), 1693–1699.

[11] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, Cambridge, 1999.

[12] D. Grigoriev, 'Testing shift-equivalence of polynomials by deterministic, probabilistic and quantum machines', *Theor. Comp. Sci.*, **180** (1997), 217–228.

[13] J. Hoffstein and D. Lieman, 'The distribution of the quadratic symbol in function fields and a faster mathematical stream cipher', *Proc. Workshop on Cryptography and Computational Number Theory, Singapore 1999*, Birkhäuser, 2001, 59–68.

[14] L. Ip, 'Solving shift problems and hidden coset problems using the Fourier transform', *Preprint*, 2002, 1–15.

[15] A. Yu. Kitaev, *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*, American Mathematical Society, 2002.

[16] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996.

[17] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[18] C. Mauduit, 'Finite and infinite pseudorandom binary words', *Theor. Comp. Sci.*, **273** (2002), 249–261.

[19] C. Mauduit and A. Sárközy, 'On finite pseudorandom binary sequences 1: Measure of pseudorandomness, the Legendre symbol', *Acta Arith.*, **82** (1997), 365–377.

[20] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2002.

[21] R. Peralta, 'On the distribution of quadratic residues and nonresidues modulo a prime number', *Math. Comp.*, **58** (1992), 433–440.

[22] J. Rivat and A. Sárközy, 'On pseudorandom binary sequences and their applications', *Preprint*, 2001, 1–18.

[23] P. Shor, 'Quantum information theory: Results and open problems,' *Geometric and Functional Analysis*, **2** (2000), 816–838.

[24] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.